UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA, v. NATHANIEL PEMBROOK, DAVID BRILEY, SHAEED CALHOUN, ORLANDO JOHNSON, Defendants.	Case No. 2:14-cr-20525 Honorable Laurie J. Michelson

OPINION AND ORDER DENYING MOTION TO SUPPRESS CELL SITE LOCATION INFORMATION [56] AND GRANTING IN PART MOTION TO EXCLUDE OR LIMIT EXPERT TESTIMONY [53]

On April 22, 2014, four men attempted to rob a jewelry store in Grand Rapids, Michigan, but, after one was shot by a store owner, they fled without merchandise. Later that same day, three men stole $1,500,000 in Rolex watches from a jewelry store in West Bloomfield, Michigan. Defendants Nathaniel Pembrook, David Briley, Shaeed Calhoun, and Orlando Johnson are charged with multiple criminal offenses arising out of these robberies (the first might have only been an attempt, but, for convenience, the Court will, as the parties do, refer to the Grand Rapids and West Bloomfield incidents as robberies). The Government believes Defendants are responsible for the robberies in part because of what it learned from data it obtained—without a warrant—from cellular-phone service providers. In particular, logs from the cell towers close by the two jewelry stores allegedly indicate that a phone used by Johnson was in the area of both stores at the time of the two robberies. Other cell-site data purportedly shows that Calhoun, Briley, and Pembrook traveled together (at least roughly) from Philadelphia, Pennsylvania, to Wisconsin, to the location of the two robberies, and then back to Philadelphia.

Calhoun says that by obtaining the cell-site data without a warrant, the Government conducted a search prohibited by the Fourth Amendment. So he moves to suppress the cell-site data. (Dkt. 56, Mot. to Suppress Cell Site Location Information.) (His motion is joined by Pembrook (Dkt. 57), Briley (Dkt. 58), and Johnson (Dkt. 59), but they provide no additional argument so the Court will refer to the motion to suppress as Calhoun's.) Calhoun also seeks to exclude from trial the testimony of the Government's cell-site data expert. (Dkt. 53, Mot. to Exclude Expert.) (The motion is again joined by Pembrook (Dkt. 55), Briley (Dkt. 58), and Johnson (Dkt. 59) without additional argument; so the Court also refers to the motion to exclude as Calhoun's.) The Court has carefully considered these two motions and listened to oral argument. For the reasons set forth below, Calhoun's motion to suppress will be DENIED and Calhoun's motion to exclude will be DENIED IN PART AND GRANTED IN PART.

I.

A.

Some background on how cellular towers communicate with cellular phones helps to understand how the Government used cell-site data to investigate the two jewelry-store robberies and the associated expert testimony the Government plans to elicit at trial.

For a cellular phone to receive a call, send a text message, or download a webpage, it must communicate with a cellular tower. (*See* Mot. to Suppress Ex. A, Gov't Apr. 28, 2014 App. for Order ¶ 5.) A cellular phone automatically searches for a signal from nearby towers and "[o]nce the phone locates a tower, it submits a unique identifier—its 'registration' information—to the tower so that any outgoing and incoming calls can be routed through the correct tower." *United States v. Powell*, 943 F. Supp. 2d 759, 767 (E.D. Mich. 2013) (citing Timothy Stapleton, Note, *The Electronic Communications Privacy Act and Cell Location Data*, 73 Brook. L.Rev.

383, 387 (2007)). "Nearby" is a relative term: it can range from a block (maybe less) to a couple miles (maybe more) depending on the tower density in the area. *See United States v. Davis*, 785 F.3d 498, 503 & n.7 (11th Cir. 2015) (en banc); *In re Application of U.S.*, 405 F. Supp. 2d 435, 437 (S.D.N.Y. 2005). Further, although a cell phone often registers with its closest tower, "a variety of factors including physical obstructions and topography can determine which tower services a particular phone." *United States v. Evans*, 892 F. Supp. 2d 949, 952 (N.D. Ill. 2012). (*See also* Gov't Apr. 28, 2014 App. for Order ¶ 5.)

Cellular service providers (e.g., Verizon Wireless) keep track of cell-phone communications with their towers (Gov't Apr. 28, 2014 App. for Order ¶ 7); courts refer to these logs as "cell-site data" or "cell-site location information" ("CSLI" for short), *see e.g.*, *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *In the Matter of the Application of the U.S.A. for an Order Authorizing Disclosure of Historical Cell Site Information*, 40 F. Supp. 3d 89 (D.D.C. 2014). Although, a cell phone "regularly communicates with cell towers in its network" even in "idle" mode, *Evans*, 892 F. Supp. 2d at 952, the Government avers that the cell-site data at issue in this case only corresponds to active cell-phone use, for example, receiving a call or sending a text, (Dkt. 72, Gov't Resp. to Request for Supp. Br. at 1). Cell-site data might also include the "sector" of a tower to which the phone connected. For example, a tower's 360 degree coverage area might be partitioned into three 120 degree sectors. (*See* Gov't Apr. 28, 2014 App. for Order ¶ 7.) *See also United States v. Jones*, 908 F. Supp. 2d 203, 207 (D.D.C. 2012).

This cell-site data permits investigators to determine the location of a cell phone at a particular time. Assume cell-cite data show that, on June 1, 2015, a cell phone using the phone number (734) xxx-1234 initiated a call via a tower located at Liberty Street and 1st Street, in Ann

Arbor, Michigan at 12:00 p.m. and terminated that call while connected with a tower located at Liberty and 5th Avenue at 12:04 p.m. With a map showing that Liberty runs east-west (with 1st Street intersecting Liberty west of 5th Avenue) and with information from the cellular-service provider that the (734) xxx-1234 account is John Smith's, this cell-site data indicates (but does not conclusively prove) that Smith's phone traveled east on Liberty (or a parallel street) in Ann Arbor just after noon on June 1, 2015. An examination of the sector information might allow further refinement of the phone's geographic location.

B.

Some legal background is also helpful to understand Calhoun's motions. The Stored Communications Act provides in relevant part, "A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) . . . when the governmental entity . . . obtains a court order for such disclosure under subsection (d) of this section." 18 U.S.C. § 2703(c)(1)(B). In turn, subsection (d) states in relevant part, "A court order for disclosure under subsection . . . (c) . . . shall issue only if the governmental entity offers specific and articulable facts showing that there are *reasonable grounds to believe* that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703 (emphasis added). Calhoun and the Government agree that a lesser showing than probable cause satisfies "reasonable grounds to believe." (*See* Mot. to Suppress at 21; Gov't Resp. at 19.) *See also Davis*, 785 F.3d at 505 (providing that § 2703(d)'s "standard is less than the probable cause standard for a search warrant").

C.

In this case, the Government obtained cell-site data without obtaining a warrant upon a showing of probable cause. Instead, it filed Stored Communications Act applications on April 28, May 22, August 5, and September 17, 2014. The Court details the four § 2703(d) applications and corresponding court orders in turn.

1.

Six days after the robberies, the Government sought an order directing a number of cellular-service providers to produce the phone numbers of the cellular devices that, around the time of the two robberies, had connected to cell towers servicing the two jewelry stores. (*See* Mot. to Suppress Ex. A, Apr. 28, 2014 Order, Attachment A at 1.)

In support of its request, the Government provided some details of the crime. It informed the reviewing magistrate judge that on April 22, 2014, around 12:30 p.m., "a jewelry store located at 4518 Plainfield Ave NW, Grand Rapids, Michigan, was robbed by four males." (Mot. to Suppress Ex. A, Gov't Apr. 28, 2014 App. at 2.) "An employee of the business shot at, and possibly hit, one of the suspects," the Government averred. (*Id.*) "After the gunfire[,] all four suspects fled without any merchandise." (*Id.*) Further, said the application, "at approximately, 5:00pm, a jewelry store located at 6637 Orchard Lake Road, West Bloomfield Township, Michigan, was robbed by three men. . . . A review of video confirms that the three suspects were also involved in the robbery earlier that day in Grand Rapids, Michigan." (*Id.* at 2–3.) The Government further informed that it "believe[d] that cell tower information in the two locations may reveal a common number that was active at each location around the time of the crime. (*Id.* at 3.) The identification of this number will aid in identifying potential suspects involved in the

robberies." (*Id.*) The Government's application also explained (somewhat briefly) how cell towers communicate with cellular devices. (*Id.* at 3–4.)

On April 28, 2014, a federal magistrate judge granted the Government's application. She found that, consistent with 18 U.S.C. § 2703(d), "the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." (Mot. to Suppress Ex. A, Apr. 28, 2014 Order at 1.) She thus ordered Metro PCS, AT&T, Verizon, Sprint, and T-Mobile to disclose "all records and other information (not including the contents of communications) about all communications made using" the cell towers providing service to the Grand Rapids store between 10:00 a.m. and 1:00 p.m. on April 22, 2014 and the towers providing service to the West Bloomfield store between 4:00 and 5:15 p.m. on April 22, 2014. (Apr. 28, 2014 Order, Attachment A at 1.) Although the magistrate judge's order included the phone numbers of each wireless device that "registered" with the towers during the two time periods (Apr. 28, 2014 Order, Attachment A at 2), the Government advises that "[t]he data at issue in this case only includes location information for the cellular device when that device is in active use, that is, when someone is sending or receiving a call or text," (Gov't Resp. to Request for Supp. Br. at 1).

2.

Almost four weeks later, on May 22, 2014, the Government filed a second § 2703(d) application. In addition to the details of the robberies set out in its first application, the Government added that on April 28, 2014, "a Court Order was obtained . . . authorizing the FBI to obtain data from cell phone towers near the two robberies at the times the robberies occurred. From that data it was determined that one telephone number was active at both locations during

[the] time frame of each robbery, (424)302-1434." (Mot. to Suppress Ex. B, Gov't May 21, 2014 App. at 4.) Thus, the Government sought "records and information" associated with the 1434 number. (*See* Mot. to Suppress Ex. B, May 21, 2014 Order, Attachment A at 1–2.)

On May 22, 2014, a federal magistrate judge found "that the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought, which include the contents of communications and other stored files, are relevant and material to an ongoing criminal investigation." (May 21, 2014 Order at 1.) (The Government informs that despite the order's reference to "contents of communications and other stored files," it obtained no content in this case. (Gov't Resp. to Request for Supp. Br. at 1.)) He thus issued an order under § 2703 directing Verizon Wireless to provide the Government with the information it sought, including "for the time period of sixty (60) days," the names and addresses of the customers or subscribers of the "Account" associated with the 1434 number, "user activity for each connection made to or from the Account," "[i]nformation about each communication sent or received by the Account," and "all data about which 'cell towers' . . . and 'sectors' . . . received a radio signal from each cellular telephone or device assigned to the Account." (May 21, 2014 Order, Attachment A at 1–2.)

3.

About a month and a half later, on or around August 5, 2014, the Government filed a third application under 18 U.S.C. § 2703. In addition to the factual proffer set out in the first two applications, the Government explained what it had learned from the account associated with 1434 number: "[Historical records for the 1434 number] show that between 4/21/2014 and 4/23/2014 [the 1434 number] had approximately 36 contacts with telephone number (872)999-0033. These records also show that both phones were calling the same two Philadelphia (PA)

telephone numbers on the day of the robberies." (Mot. to Suppress Ex. C, Gov't Aug. 5, 2014 App. ¶ 4.) The application further explained, "Investigation to date has identified two men from Philadelphia that were involved in the robberies. The FBI believes that telephone number (872)999-0033 was involved in the above described robberies and the cell site locations this phone used will help identify the suspects involved in the crimes." (*Id.*)

On August 5, 2014, a federal magistrate judge entered an order granting the Government the right to obtain cell-site data associated with the 0033 number. (Mot. to Suppress Ex. C, Aug. 5, 2014 Order.) Consistent with § 2703(d), the judge found that the Government had "offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought, which include the contents of communications and other stored files, are relevant and material to an ongoing criminal investigation." (Aug. 5, 2014 Order at 1.) She thus ordered that, "for the time period April 21, 2014 through May 21, 2014," T-Mobile was to disclose to the Government, among other information, the names and addresses of the customers or subscribers of the "Account" associated with the 0033 number, "user activity for each connection made to or from the Account," "[i]nformation about each communication sent or received by the Account," and "all data about which 'cell towers' . . . and 'sectors' . . . received a radio signal from each cellular telephone or device assigned to the Account." (Aug. 5, 2014 Order, Attachment A at 1–2.)

4.

About six weeks later, on September 17, 2014, the Government filed the fourth § 2703 application at issue in this case. This application provided an investigation background similar to that set forth in the Government's prior application, but further explained: "Surveillance video from the two robberies and from a gas station in Michigan were reviewed by law enforcement.

Two men, Shaheed Calhoun and David Briley, were identified from these videos as being two of the members of the group that conducted the robberies." (Mot. to Suppress Ex. D, Gov't Sept. 17, 2014 App. ¶ 5.) The application continued, "Through recorded prison calls it was discovered that Calhoun was using telephone number 610-427-1641 during the time frame of the robberies. The FBI believes that telephone number 610-427-1641 was involved in the . . . robberies and the cell site locations this phone used will help identify the suspects involved in the crimes." (*Id.*)

On September 17, 2014, a federal magistrate judge entered an order similar to those entered on May 22 and August 5, 2014. Again applying the § 2703(d) standard, the judge found that the United States had "offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought, which include the contents of communications and other stored files, are relevant and material to an ongoing criminal investigation." (Mot. to Suppress Ex. D, Sept. 17, 2014 Order at 1.) She thus ordered T-Mobile to disclose, "for the time period April 15, 2014 through May 30, 2014," the names and addresses of the customers or subscribers of the "Account" associated with the 1641 number, "user activity for each connection made to or from the Account," "each communication sent or received by the Account," and "all data about which 'cell towers' . . . and 'sectors' . . . received a radio signal from each cellular telephone or device assigned to the Account." (Sept. 17, 2014 Order, Attachment A at 1–2.)

* * *

To summarize the Government's use of cell-site data in this case, it first obtained data associated with the towers around the site of the two robberies and determined that the cell phone with the number (424) 302-1434 connected to towers in the vicinity of the Medawar's jewelry store in Grand Rapids, Michigan around 12:30 p.m. and the Tapper's jewelry store in West

Bloomfield, Michigan around 5:00 p.m. The Government then sought records associated with the 1434 number, which the Government now says was Defendant Johnson's (Gov't Resp. to Mot. to Suppress at 1 n.1), and determined that the 1434 number had frequently called (872) 999-0033 around the time of the two robberies and that both those numbers had called two Philadelphia numbers. So the Government sought cell-site data from April 21 to May 21, 2014 for the 0033 number, which the Government now believes was used by Calhoun. Then, based on surveillance video, the Government concluded that Calhoun and Briley were involved in the robberies and, based on recorded prison conversations, that Calhoun had used the number (610) 427-1641 during the time of the robberies. So the Government sought cell-site data from April 15 to May 30, 2014 for the 1641 number.

From this data, it appears that the Government could determine Calhoun's approximate location between April 15 and May 30, 2014, a six-week period, and Johnson's approximate location for an eight-week period.

D.

At trial, the Government intends to call Christopher Hess, a special agent with the FBI, to testify about his analysis of the cell-site data obtained during the Government's investigation.

Pursuant to Federal Rule of Criminal Procedure 16, on April 6, 2015, the Government sent Defendants' counsel a letter summarizing Hess' testimony. The letter explained, "SA Hess will specifically testify to cell site location data for four cell phones for the period of April 18 – 23, 2014. Using call detail records provided by the telecommunication companies that include information related to the cellular towers that a particular cellular telephone is communicating with, SA Hess will plot out the locations of the four cellular phones from April 18 – 23, 2014."

(Mot. to Exclude Expert Ex. A, Apr. 6, 2015 Letter from Graveline to Defendants' Counsel at 1.) The letter identified four phone numbers and their alleged users:

1. (267) 506-7819 – user David Briley
2. (424) 302-1434 – user Orlando Johnson
3. (872) 999-0033 – user Shaheed Calhoun
4. (215) 526-1574 – user [unidentified male] #1

(Apr. 6, 2015 Letter from Graveline to Defendants' Counsel at 2.) (The 1434 and 0033 numbers were the subject of § 2703 orders discussed above, but the 7819 and 1574 numbers were not.)

The Government's April 6, 2015 letter also attached a document titled "Basic Principals [*sic*] Utilized in Record Analysis" prepared by Hess. In it, Hess provides how cell phones communicate with cell towers. Much of the information is similar to that presented above, but Hess included some additional detail about cellular communications. For example, "The phone 'sees' other towers around the SERVING CELL and will constantly measure those signal strengths. However the phone will not randomly reselect to an adjacent tower unless the tower is on its 'neighbor list' which is controlled by the network service provider," and "As the phone moves, it will choose a new serving cell based on signal strength and neighbor list. If this occurs while the phone is in a call, the phone will 'handoff' the call to the next cell site/sector." (Apr. 6, 2015 Letter from Graveline to Defs.' Counsel at 3.)

The letter also included four maps prepared by Hess—one for each of the four phone numbers referenced in the Government's letter. (Apr. 6, 2015 Letter from Graveline to Defs.' Counsel at 4.) Each map shows data points at Philadelphia, Pennsylvania, South Bend, Indiana, Grand Rapids, Michigan, and West Bloomfield, Michigan. (*Id.*) Underneath the maps, Hess wrote three statements: "Preliminary analysis identified similar travel patterns of the referenced

numbers"; "Travel originated and terminated in Philadelphia, PA"; and "The phones traveled to WI then to MI and utilized towers consistent with the geographic area encompassing robbery locations in Grand Rapids and Southfield, Michigan." (*Id.*)

Finally, the Government's Rule 16 letter included Hess' curriculum vitae. (Apr. 6, 2015 Letter from Graveline to Defs.' Counsel at 5.) It states, among other things, that Hess is educated in criminal justice and has received over 400 hours of training in various cellular protocols and radio frequency theory. (*Id.*) The Government informs that "Hess has testified as an expert in historical cell site analysis in over 25 criminal trials," including before five different judges of this judicial district. (Gov't Resp. to Mot. to Exclude Expert at 7.)

II.

The Court starts with Calhoun's motion to suppress. Calhoun argues that the cell-site data obtained pursuant to the April 28, 2014 order entered pursuant to 18 U.S.C. § 2703(d) must be suppressed because that section of the Stored Communications Act does not permit the Government to obtain "cell tower dump data." (Mot. to Suppress at 22–24.) Calhoun further argues that the evidence obtained pursuant to the April 28, August 5, and September 17, 2014 orders must be suppressed as unreasonable searches prohibited by the Fourth Amendment. (Mot. to Suppress at 9–22.) (Calhoun does not explicitly seek to suppress the evidence obtained pursuant to the May 22, 2014 order for the 1434 number (*see* Mot. to Suppress at 9–22), presumably because the Government believes that number was used by Johnson.) The Court addresses these arguments in turn.

A.

Calhoun's argument that the Government violated the Stored Communications Act by applying for and obtaining an order directing AT&T, Verizon Wireless, and other cellular-

service providers to produce a log of all cellular devices that registered with cellular towers close by the jewelry stores around the time of the two robberies is based on the text of the Act. (Mot. to Suppress at 23–24.) He focuses on the following language: "A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to *a subscriber to or customer of* such service (not including the contents of communications) . . . ." 18 U.S.C. § 2703(c) (emphasis added); *see also* 18 U.S.C. § 2702(c)(1) ("A provider described in subsection (a) may divulge a record or other information pertaining to *a subscriber to or customer of* such service . . . ." (emphasis added)). Calhoun concludes that Congress' use of the singular "a subscriber" means that the Act "does not authorize a request for records pertaining to a large set of unidentified persons. . . . To rule otherwise is to conclude that Congress intended to authorize broad-based requests for information about potentially thousands of people by using language plainly limited to a single person." (Mot. to Suppress at 24.)

This argument is not novel and has been rejected by other district courts. *See In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d)*, 42 F. Supp. 3d 511, 513 (S.D.N.Y. 2014); *In re Cell Tower Records Under 18 U.S.C. 2703(d)*, No. H-15-136M, 2015 WL 1022018, at *3 (S.D. Tex. Mar. 9, 2015).

But even accepting Calhoun's interpretation of § 2703, the Court cannot grant him the relief he seeks. Calhoun asserts that because obtaining a tower dump is not permissible under the Stored Communications Act, the Court "must . . . suppress[]" that data. (Mot. to Suppress at 24–25.) Not so. The Act lists remedies for violations of its provisions, none of which is suppression. *See* 18 U.S.C. §§ 2701(b), 2707; *United States v. Clenney*, 631 F.3d 658, 667 (4th Cir. 2011) (providing that "[t]here is no mention of a suppression remedy" for violations of § 2703(c)). And

the Act says, "The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. So the Court cannot suppress the tower dump data even if the Government violated the Secured Communications Act by obtaining it. *See United States v. Corbitt*, 588 F. App'x 594, 595 (9th Cir. 2014); *United States v. Powell*, 444 F. App'x 517, 520 (3d Cir. 2011).

B.

Calhoun's primary argument is that the Court must suppress the cell-site data that the Government obtained pursuant to the April 28, August 5, and September 17, 2014 orders because that data was obtained via a search prohibited by the Fourth Amendment.

The Fourth Amendment to the United States Constitution provides, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." A "search[]" within the meaning of the Amendment occurs when "Government physically occupie[s] private property for the purpose of obtaining information." *See United States v. Jones*, — U.S. —, 132 S. Ct. 945, 949, 181 L. Ed. 2d 911 (2012). And, under *Katz v. United States*, 389 U.S. 347 (1967), a "search" also occurs "when the government infringes upon an expectation of privacy that society is prepared to consider reasonable." *See Smith v. Maryland*, 442 U.S. 735, 740 (1979); *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010).

Calhoun relies on the latter formulation. Combining the two concurring opinions in *United States v. Jones*, — U.S. —, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012), Calhoun asserts that five justices believe that people have a legitimate expectation of privacy in their hour-by-hour whereabouts over an extended period, such as the six- and eight-week periods at issue in this case. (Mot. to Suppress at 10–13, 17–19.); *see also United States v. Maynard*, 615 F.3d 544,

562 (D.C. Cir. 2010) *aff'd in part sub nom. Jones*, 132 S. Ct. 945 ("A person who knows all of another[']s travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups[.]" (footnote omitted)). And citing *United States v. Karo*, 468 U.S. 705 (1984), Calhoun also argues that cell-site data has the potential to reveal information about a person's home and is thus shielded from warrantless searches by the Fourth Amendment. (Mot. to Suppress at 11–12, 13–14.) Finally, citing *United States v. Knotts*, 460 U.S. 276 (1983), Calhoun argues that because potentially hundreds of wireless devices were connected to the towers proximate to the two jewelry stores around the time of the robberies, the "cell tower [data] dump" obtained pursuant to the April 28, 2014 order was a "dragnet" search that violated the Fourth Amendment. (Mot. to Suppress at 15–16.)

It is not necessary to directly address these arguments. The question presented is whether the cell-site evidence the Government has already obtained should be suppressed, not whether an application for that data should be granted. And suppression is not an automatic remedy for a Fourth Amendment violation. *Herring v. United States*, 555 U.S. 135, 140 (2009). The Supreme Court has directed lower courts to ensure that suppression will have "[r]eal deterrent value" and to be mindful that the "bottom-line effect [of exclusion], in many cases, is to suppress the truth and set the criminal loose in the community without punishment." *Davis v. United States*, — U.S. —, 131 S. Ct. 2419, 2426, 180 L. Ed. 2d 285 (2011) (citation and internal quotation marks omitted). The balance has been articulated this way: When law enforcement "exhibit[s] deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs," but when law enforcement "act[s] with an objectively reasonable good-faith belief that their conduct is

lawful . . . the deterrence rationale loses much of its force, and exclusion cannot pay its way." *Id.* at 2427–28 (internal quotation marks omitted). Suppression is a remedy of "last resort." *Id.* at 2527.

As will be explained, at the time the Government obtained the cell-site data at issue in this case, there was no binding authority holding that obtaining cell-site data, even cell-site data revealing an individual's whereabouts over an extended period or his presence in a private place, required a warrant supported by probable cause. Further, as will also be explained, the persuasive authority available at the time was mixed. As such, the Court finds that the Government could not have been "deliberate, reckless, or grossly negligent," *Davis*, 131 S. Ct. at 2427, in violating Calhoun's Fourth Amendment rights (assuming, without deciding, that it did violate them).

1.

The Court starts with the Supreme Court cases that should have informed the FBI and the United States Attorney's decision to obtain the month-and-a-half of data associated with Calhoun's cell-phone accounts.

In *United States v. Miller*, 425 U.S. 435 (1976), government agents were investigating Mitchell Miller for tax fraud and, without a warrant, obtained records from two of Miller's bank accounts. *See id.* at 436–38. One bank gave the agents "all checks, deposit slips, two financial statements, and three monthly statements." *Id.* at 438. The Supreme Court, applying *Katz*'s reasonable-expectation-of-privacy test, held that the agents had not violated Miller's Fourth Amendment rights in obtaining the bank records. The Court explained that "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* at 442. Said the Court: "The depositor takes the risk, in revealing his affairs to

another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443 (citation omitted).

Smith v. Maryland, 442 U.S. 735 (1979), rests on the same voluntary-disclosure doctrine. There, police suspected Michael Lee Smith of a robbery and so they, without a warrant, directed his telephone company to install "a pen register at its central offices to record the numbers dialed from the telephone at [Smith's] home." *Id.* at 737. Not long thereafter, the pen registered that Smith had dialed the robbery victim's number; "[o]n the basis of [that] and other evidence, the police obtained a warrant to search [Smith's] residence" where it found further evidence linking Smith to the robbery. *Id.* The Court held that "even if [Smith] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation [was] not 'one that society is prepared to recognize as reasonable.'" *Id.* at 743 (quoting *Katz*, 389 U.S. at 361). In accord with *Miller*, the Court reasoned, "When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed." *Id.* at 744.

United States v. Knotts, 460 U.S. 276 (1983), held that law enforcement's warrantless tracking was permissible but under a slightly different rationale than that of *Miller* and *Smith.* In *Knotts*, police placed a "beeper" inside a chloroform drum to track, via a radio signal, the movements of individuals suspected of manufacturing drugs. *Id.* at 277–78. In the course of tracking the suspects, the police lost the beeper signal, and when they picked it up, the signal was

stationary at a cabin. *Id.* at 278. "Relying on the location of the chloroform derived through the use of the beeper and additional information obtained during three days of intermittent visual surveillance of [the] cabin, officers secured a search warrant," executed it, and discovered a drug laboratory. *Id.* at 279. The Supreme Court held that the officers' use of the beeper without a warrant did not offend the Fourth Amendment. In the language of *Katz*, the Court explained, a "person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* at 281. In responding to the argument that the beeper had reached the premises of a private dwelling, the Court was careful to note that there was no evidence "that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin." *Id.* at 285. In response to the argument that the beeper would allow the police to engage in 24-hour surveillance, the Court explained, "if such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 284.

United States v. Karo, 468 U.S. 705 (1984), also involved the authorities' use of a beeper, but, unlike *Knotts*, "present[ed] the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence." *Id.* at 714. The DEA had installed a beeper inside a can of ether it thought would be used to manufacture drugs. *Id.* at 708. The DEA tracked the can to a house, but "did not maintain tight surveillance [of the residence] for fear of detection." *Id.* at 709. After the suspects left the house, and again on the following day, agents used the beeper to determine that the can of ether was still in the home. *Id.* at 710. In

holding the DEA's warrantless use of the beeper unconstitutional, the Supreme Court characterized as "obvious" the fact that "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable." *Id.* Given that the Government's use of the beeper "reveal[ed] a critical fact about the interior of the premises" that the Government "could not have otherwise obtained without a warrant," the warrantless use of the beeper to determine the presence of the can in the house ran afoul of the Fourth Amendment. *Id.* at 715, 718; *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001) ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search—at least where (as here) the technology in question is not in general public use." (internal quotation marks and citation omitted)).

United States v. Jones, — U.S. —, 132 S. Ct. 945, 951, 181 L. Ed. 2d 911 (2012), involves much more recent technology: government agents installed a Global-Positioning-System tracking device "on the undercarriage of the Jeep" and, over a 28-day period, tracked the vehicle's movements to within 50 to 100 feet. 132 S. Ct. at 947. This ultimately led to Jones being indicted for conspiracy to distribute cocaine. *Id.* at 948. The Justices authored three opinions. The majority opinion, authored by Justice Scalia and joined by four other justices, focused on the pre-*Katz* physical-intrusion-of-property test and "h[e]ld that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitute[d] a 'search.'" *Id.* at 949. Justice Alito instead analyzed the issue under *Katz*'s legitimate-expectation-of-privacy test. In his and three other justices' view, "relatively short-term monitoring of a person's movements on public streets accords with

expectations of privacy that our society has recognized as reasonable." *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in judgment). "But," said Justice Alito, "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* He explained, "For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* Although Justice Alito acknowledged that the line between short- and long-term monitoring might be blurry, for him (and the three justices who joined his opinion) "the line was surely crossed before the 4–week mark." *Id.* Justice Sotomayor wrote a concurrence. Although she joined Justice Scalia's opinion in full (thereby making Justice Scalia's opinion a true majority opinion), she wrote, "I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" *Jones*, 132 S. Ct. at 955 (Sotomayor, J.) (quoting *Jones*, 132 S. Ct. at 964 (Alito, J.)).

Even charging the Government with complete knowledge of all these Supreme Court decisions, the Court cannot conclude that the Government's decision to obtain cell-site data associated with Calhoun's cellular accounts without a warrant was a "deliberate, reckless, or grossly negligent disregard for [Calhoun's] Fourth Amendment rights." *Davis*, 131 S. Ct. at 2427–28 (internal quotation marks omitted).

Starting with *Knotts*, if the Government had good reason to believe that the cell-site data it would obtain would only reveal Calhoun's location on the "public thoroughfares" in and between Philadelphia, Grand Rapids, and West Bloomfield, then the Government would also have had good reason to believe that Calhoun did not have a reasonable expectation of privacy in the cell-site data. And that was the case for the initial April 28, 2014 "tower dump" as the towers

at issue serviced the two commercial jewelry stores. Defendants had no legitimate expectation of privacy there; and Defendants have not suggested that they had any expectation of privacy in nearby buildings (which, presumably, were mostly commercial in nature). As for the fact that the tower dump may have disclosed the approximate location of hundreds of cell phone users, Defendants have not explained how they can complain about a potential intrusion on privacy interests not their own. *See United States v. Noble*, 762 F.3d 509, 526 (6th Cir. 2014) ("It is long-settled that 'Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted.'" (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969))). Nor did *Knotts*, as Calhoun suggests, prohibit this type of broad-sweeping search; all the Supreme Court said was "*if* such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Knotts*, 460 U.S. at 284 (emphasis added).

More importantly, the voluntary-disclosure reasoning of *Miller* and *Smith* supports the Government's decision to proceed without a warrant—assuming that, by mid-2014, people understood that their cellular phones sent data to cellular towers to make calls, send texts, or download webpages. This assumption would not have been unreasonable for the Government to make. *See In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 614 (5th Cir. 2013) ("Because a cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he voluntarily conveys his cell site data each time he makes a call."); *In re Application of the U.S.A.*, 42 F. Supp. 3d 511, 517 (S.D.N.Y. 2014) ("Many courts have held that [the] voluntary disclosure doctrine (also known as the 'third-party disclosure doctrine') [set out

in *Smith* and *Miller*] compels the conclusion that the Government's acquisition of cell site location data is not a 'search' within the meaning of the Fourth Amendment."); *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129, 137–42 (E.D.N.Y. 2013) (providing a number of reasons for why cellular phone users should understand that cellular-phone service providers log geolocation information and that "all of the known tracking technologies may be defeated by merely turning off the phone"); *but see In re Application of U.S.*, 620 F.3d 304, 317–18 (3d Cir. 2010) (concluding that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way" and that "it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information" (citations omitted)); *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 756–57 (S.D. Tex. 2005) ("Unlike dialed telephone numbers, cell site data is not 'voluntarily conveyed' by the user to the phone company. As we have seen, it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge.").

And the fact that the Government could have reasonably thought that the voluntary-disclosure rationale articulated in *Smith* and *Miller* applied to the cell-site data it sought, could have reduced the weight of *Karo* in the Government's mind. As the Fifth Circuit explained in an opinion issued before the events of this case: "Both *Karo* and *Smith* involved the Government's acquisition of information about the interior of a home: that a particular canister was located in the home or that a person was calling particular numbers from a phone in the home. But in *Karo* (as in *Jones*), the Government was the one collecting and recording that information. And this is the distinction on which the Government's affirmative argument turns." *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 609 (5th Cir. 2013); *see also In re Application*

of the U.S.A., 42 F. Supp. 3d 511, 518 (S.D.N.Y. 2014) ("As *Smith* makes clear, the voluntary disclosure doctrine applies even where the disclosures are made from the protected space of the home.").

Regarding *Jones*, the possibility that Justice Sotomayor's opinion could be read as a fifth vote for the finding that society is willing to accept as reasonable a person's claim to privacy in their cumulative whereabouts does not show that the Government acted with reckless disregard to Calhoun's Fourth Amendment rights. Although Justice Sotomayor did say she "agree[d] with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy,'" *Jones*, 132 S. Ct. at 955 (Sotomayor, J.) (quoting *Jones*, 132 S. Ct. at 964 (Alito, J.)), her concurrence was not unequivocal on that point. Noting that "GPS monitoring generates a precise, comprehensive record of a person's public movements," and that GPS monitoring comes at little cost to the government (as compared to traditional means of surveillance), Justice Sotomayor stated that she "*would*" take those attributes "into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements." *Id.* at 956 (emphasis added). And in discussing *Smith*'s voluntary-disclosure doctrine, Justice Sotomayor used similar some-day language: that it "*may*" be necessary to revisit "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Id.* at 957 (emphasis added). All of this is underscored by her conclusion: "Resolution of these difficult questions in this case is *unnecessary*, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision. I therefore join the majority's opinion." *Id.* at 957 (emphasis added). Thus, the Government could have reasonably understood that only four justices had settled on the position that people have a reasonable expectation of privacy in their whereabouts over the

long term (where there is no issue regarding public disclosure of the information gleaned from the tracking method). *See also United States v. Davis*, 785 F.3d 498, 500 (11th Cir. 2015) (en banc) (finding that in *Jones* Justice Sotomayor raised the question of whether *Smith* might need to be revisited "but did not even purport to answer it." (quoting *Jones*, 132 S. Ct. at 957)); *United States v. Herron*, 2 F. Supp. 3d 391, 402 (E.D.N.Y. 2014) ("*Jones* does not appear to have substantially altered the state of the law as to historical cell-site records.").

In short, no Supreme Court authority established by mid-2014 that obtaining cell-site data—even data that might reveal Calhoun's daily travel over a six-week period or disclose his presence in a private place—was a search within the meaning of the Fourth Amendment. Thus, the Government's decision to proceed without a warrant was not in reckless disregard to any Supreme Court precedent such that suppression of the data would be the appropriate remedy.

2.

The Court next considers binding Sixth Circuit precedent and asks whether that body of law made clear to the government that obtaining cell-site data without a warrant was unconstitutional. Several opinions are relevant.

In *United States v. Forest*, 355 F.3d 942 (6th Cir. 2004), *judgment vacated on other grounds*, 543 U.S. 1100 (2005), DEA agents identified Craig Forest and Herman Garner as "active cocaine traffickers." *Id.* at 947. Although the agents conducted physical surveillance of Forest and Garner, they "were unable to maintain constant visual contact." *Id.* "In order to reestablish visual contact, a DEA agent dialed Garner's cellular phone (without allowing it to ring) several times that day and used Sprint's computer data to determine which cellular transmission towers were being 'hit' by Garner's phone. This 'cell-site data' revealed the general location of Garner." *Id.* The Sixth Circuit found the facts similar to those of *Knotts*: "Garner

acknowledges that the cell-site data was used to track his movements only on public highways. The rationale of *Knotts* therefore compels the conclusion that Garner had no legitimate expectation of privacy in the cell-site data because the DEA agents could have obtained the same information by following Garner's car." *Id.* at 951. Notably, Garner "persuasively distinguishe[d]" the Supreme Court's decision in *Smith* by arguing that unlike the robbery suspect in that case who voluntarily called his victim from his home, "he did not use his telephone"; instead, "[t]he *agent dialed* Garner's phone number and the dialing caused Garner's phone to send out signals." *Id.* Still, the Sixth Circuit thought that while Garner's argument "might have merit in other contexts," it had no significance on the facts before it because "the cell-site data [was] simply a proxy for Garner's visually observable location" and "Garner had no legitimate expectation of privacy in his movements along public highways." *Id.* at 951.

United States v. Skinner, 690 F.3d 772 (6th Cir. 2012), involved facts very similar to those of *Forrest* and the Sixth Circuit again found *Knotts* controlling. Melvin Skinner was suspected of working as a marijuana courier. *Id.* at 775–76. Authorities repeatedly "pinged" Skinner's phone, which allowed them to determine that he was travelling "on Interstate 40 across Texas." *Id.* at 776. This tracking eventually informed law enforcement that Skinner had stopped at a truck stop near Abilene, Texas. DEA agents were dispatched to the stop and a search of the motorhome Skinner was driving uncovered 1,100 pounds of marijuana. *Id.* at 776. Skinner sought to suppress the search of the motorhome, asserting that "the agents' use of GPS location information emitted from his cell phone was a warrantless search that violated the Fourth Amendment." *Id.* at 776. The Sixth Circuit disagreed: "Similar to the circumstances in *Knotts*, Skinner was traveling on a public road before he stopped at a public rest stop. While the cell site information aided the police in determining Skinner's location, that same information could have

been obtained through visual surveillance." *Id.* at 778. In reference to Justice Alito's opinion in *Jones*, the Sixth Circuit stated, "There may be situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes." *Id.* at 780. But, said our Court of Appeals, "No such extreme comprehensive tracking [was] present in this case. . . . [T]he DEA agents only tracked Skinner's cell phone for three days." *Id.*

The government personnel involved here could have reasonably read *Forest* and *Skinner* as providing little guidance beyond *Knotts* and *Jones*. In particular, because the Sixth Circuit found that the cell-site data obtained in *Forest* and *Skinner* could have been obtained through traditional tracking on the public roadways, it found that *Knotts* controlled. True, in *Forest*, the Sixth Circuit indicated that *Smith*'s voluntary-disclosure doctrine might not apply to the situation when a cell-phone is merely registered to a tower but in "idle" (or merely receives calls but does not make them), but the Court of Appeals did not decide that issue. It instead found *Knotts*' public-thoroughfare doctrine a narrower decisional ground, reasoning that the defendant's argument "*might* have merit in other contexts." 355 F.3d at 951 (emphasis added). As for *Skinner*, it is true that the Sixth Circuit indicated that it might follow Justice Alito's reasoning in *Jones* where the Government comprehensively tracks a person's movements. But like Justice Sotomayor in *Jones*, our Court of Appeals did not unequivocally make that finding—*Knotts* disposed of the appeal.

At oral argument, it became apparent that Calhoun's primary authority against the application of a good-faith exception in this case is *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). But that case is far afield of this one. True, it involved a motion to suppress data that the Government obtained pursuant to the Stored Communications Act. *Id.* at 282. But the data at

issue in *Warshak* was the *content* of email messages—not, for example, data indicating from which internet-protocol address a message was sent. *See id.* (noting Government's seizure of 27,000 private emails). Indeed, the Sixth Circuit's "hold[ing]" was that "a subscriber enjoys a reasonable expectation of privacy in the *contents* of emails that are stored with, or sent or received through, a commercial ISP." *Id.* at 288 (emphasis added) (internal quotation marks omitted). Here, the Government did not obtain the content of Calhoun's text messages or cell-phone conversations.

In sum, even charging the FBI and the United States Attorney with knowledge of relevant Sixth Circuit precedent, the Court cannot say that the Government recklessly disregarded Calhoun's Fourth Amendment rights in obtaining the cell-site data Calhoun seeks to suppress.

3.

A consideration of persuasive authority does not alter the Court's conclusion.

Starting with an examination of the precedent from this judicial district available as of mid-2014, nothing the Court could find clearly informed the Government that obtaining historical cell-site data without a warrant was unlawful. The closest would have been *United States v. Powell*, 943 F. Supp. 2d 759 (E.D. Mich. 2013)—but that case involved real-time tracking of an individual's whereabouts via cell-site data. *Id.* at 770 (holding "that when the government requests authorization to engage in long-term, real-time tracking of an individual's movements via his or her cell phone, the situation reaches past the law set forth in *Skinner*, and Fourth Amendment concerns are implicated" and providing that, with regard to real-time data, a "significant majority" of courts have required a warrant). Although this Court questions whether the historical versus real-time distinction makes a constitutional difference, at least some courts had found it significant. *United States v. Graham*, 846 F. Supp. 2d 384, 391 (D. Md. 2012); *In re*

Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d), 509 F. Supp. 2d 76, 80 (D. Mass. 2007). Thus, the Court cannot say that one non-binding case to the contrary shows that the Government acted recklessly in proceeding by order and not warrant. Indeed, another case from this district on the books in mid-2014 lent some support to the Government's action. *See United States v. Carpenter*, No. 12-20218, 2013 WL 6385838 (E.D. Mich. Dec. 6, 2013) (rejecting argument that a cell phone user's reasonable expectation of privacy in prolonged surveillance data demonstrated that the Stored Communications Act "reasonable grounds" standard was unconstitutional).

Moreover, the out-of-district persuasive authority available at the time of the Government's four § 2703(d) applications was far from one-sided. *Compare In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir. 2013) (finding the defendant had no reasonable expectation of privacy in sixty days of cell-site data revealing the defendant's approximate geographic location when phone was used (and not merely in idle) because using a cell phone is "entirely voluntary" and "the Government does not . . . require [someone] to make a call, let alone to make a call at a specific location"); *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129, 131–32, 146 (E.D.N.Y. 2013) (finding, no reasonable expectation of privacy in 30 days' worth of prospective geolocation data; reasoning, "it is clearly within the knowledge of cell phone users that their telecommunication carrier, smartphone manufacturer and others are aware of the location of their cell phone at any given time. . . . [I]ndividuals who do not want to be disturbed by unwanted telephone calls at a particular time or place simply turn their phones off, knowing that they cannot be located"); *United States v. Graham*, 846 F. Supp. 2d 384, 387, 391 (D. Md. 2012) (finding, where government sought cell-site data covering "two hundred and twenty-one days" and included "20,235 individual cell site

location data points" that defendants did "not have a legitimate expectation of privacy in the historical cell site location records acquired by the government"), *with United States v. Davis*, 754 F.3d 1205, 1215 (11th Cir. 2014) (finding, where government obtained 67 days of records showing "the telephone numbers for each of Davis's calls and the number of the cell tower that connected each call," that "the government's warrantless gathering of [Davis's] cell site location information violated his reasonable expectation of privacy"), *opinion vacated*, 573 F. App'x 925 (11th Cir. 2014);[1] *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 312–13 (3d Cir. 2010) (relying on *Knotts* to find that probable cause was not necessary to obtain historical CSLI where there was "no evidence in this record that historical CSLI" extended to people's homes, but rejecting the notion that *Smith*'s voluntary-disclosure doctrine applied to cell phone use); *In the Matter of an Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 116 (E.D.N.Y. 2011) (finding that a request for prolonged historical cell-site constituted a "search" under the Fourth Amendment that required a warrant and a showing of probable cause).

Indeed, it may have been that at the time of the Government's applications in this case, a majority of courts had held that law enforcement could obtain historical cell-site data without a warrant. *See United States v. Moreno-Nevarez*, No. 13-CR-0841-BEN, 2013 WL 5631017, at *2 (S.D. Cal. Oct. 2, 2013) (joining "the majority of the courts to address this issue . . . in concluding that there is no 'reasonable expectation of privacy' in historical cell site data" in case where government sought two-and-a-half months of historical cell-site data generated only when

[1] The Court recognizes that this panel decision in *Davis* was vacated on September 4, 2014, after the Government filed three of the four § 2703(d) applications at issue in this case. And while it was nullified by the en banc court, it could have been relevant to the Government's decision-making at least as to those three applications.

the user made or received a call); *Graham*, 846 F. Supp. 2d at 389 (reviewing cases from 2010 and 2011 and concluding that "[a] majority of courts . . . have concluded that the acquisition of historical cell site location data pursuant to the Stored Communications Act's specific and articulable facts standard does not implicate the Fourth Amendment, regardless of the time period involved."). *But cf. United States v. Powell*, 943 F. Supp. 2d 759, 770 (E.D. Mich. 2013) (providing that, with regard to real-time prospective data, a "significant majority" of courts have required a warrant).

Given the split in persuasive authority at the time the Government acted, even charging the Government with knowledge of cases finding or suggesting that a warrant was required to obtain the cell-site data associated with Calhoun's accounts, the Court cannot say that the Government recklessly disregarded Calhoun's Fourth Amendment rights by proceeding without a warrant.

4.

Before concluding the deterrence analysis, the Court makes two further points.

First, with limited exceptions, "[t]he exclusionary rule does not bar the government's introduction of evidence obtained by police officers acting in objectively reasonable reliance on a search warrant that is subsequently invalidated." *United States v. McPhearson*, 469 F.3d 518, 525 (6th Cir. 2006) (internal quotation marks omitted). Although a magistrate judge did not issue a warrant in this case, two magistrate judges did issue § 2703(d) orders granting the Government the right (or, at least the perceived right) to obtain the cell-site data it sought. This lends some support to the Government's claim that it proceeded in good faith. *See United States v. Jones*, 908 F. Supp. 2d 203, 215 (D.D.C. 2012) ("Here, Magistrate Judge Facciola—and later Magistrate Judge Kay—considered the government's applications and determined that the

government could obtain prospective cell-site information under 18 U.S.C. § 2703(c) and had satisfied the standard set forth in § 2703(d). . . . [I]t was objectively reasonable for the government to rely on the independent judicial determinations that no warrant was required."); *United States v. Ferguson*, 508 F. Supp. 2d 7, 9 (D.D.C. 2007) ("The fact that a neutral Magistrate Judge approved the Government's applications under the SCA provides further reason to deem the Government's reliance on the SCA to be objectively reasonable.").

The second point involves Calhoun's primary argument that suppression in this case will result in significant deterrence: that, as opposed to cases where police perform a search in haste, this case involved a deliberate decision by a United States Attorney, someone with a deeper understanding of Fourth Amendment jurisprudence. (*See* Mot. to Suppress at 21; Reply to Gov't Resp. to Mot. to Suppress at 6.) Whatever merit this argument has, the Court's analysis has proceeded under the assumption that the United States Attorney knew all of the authorities cited above. So Calhoun's argument does not disturb the Court's analysis.

* * *

The point of suppression is deterrence; and when the Government "act[s] with an objectively reasonable good-faith belief that their conduct is lawful . . . the deterrence rationale loses much of its force, and exclusion cannot pay its way." *Davis*, 131 S. Ct. at 2426–48. That is the case here: no binding precedent dictated that the Government needed a warrant to obtain the cell-site data that Calhoun seeks to suppress and persuasive authority on the issue was mixed, or, arguably, favored proceeding without a warrant. As such, the Court will deny Calhoun's motion (joined in by the other Defendants) to suppress the cell-site data that the Government obtained during its investigation.

III.

Remaining for resolution is Calhoun's motion to exclude the Government's cell-site data expert, Christopher Hess, from testifying at trial or, in the alternative, to limit his testimony, or, in further alternative, for additional discovery relating to Hess' testimony.

Calhoun raises four arguments. First, he says that the Government's Federal Rule of Criminal Procedure 16 letter and the accompanying report by Hess "fail[] to provide any details describing the bases and reasons" for Hess' conclusions, thereby depriving the Court of the ability to determine whether his methods are reliable. (Dkt. 53, Mot. to Exclude Expert at 9.) Second, Calhoun says that Hess' opinion is based on the "theory of granulization"— a theory untested by the scientific community. (Mot. to Exclude Expert at 10–11; Reply re Mot. to Exclude Expert at 3.) Third, Calhoun argues that Hess' testimony is not admissible under Federal Rule of Evidence 701 as lay-witness testimony. (*Id.* at 11–13.) Finally, Calhoun asserts that if the Court allows Hess to testify, he would like additional discovery so that he can effectively cross-examine Hess at trial. (*Id.* at 14.)

The Court begins with Calhoun's third point because the Government agrees with it: the Government acknowledges that Hess' testimony is not lay-witness testimony and so Hess must pass this Court's screening of expert witnesses. (*See* Gov't Resp. to Mot. to Exclude Expert at 4–8.) So the question is whether Hess' testimony satisfies the standards set out in Federal Rule of Evidence 702 and *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579 (1993).

Federal Rule of Evidence 702 provides:

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
>
> (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;

(b) the testimony is based on sufficient facts or data;

(c) the testimony is the product of reliable principles and methods; and

(d) the expert has reliably applied the principles and methods to the facts of the case.

Fed. R. Evid. 702. Or more concisely stated, the question is whether Hess' expert opinion "rests on a reliable foundation and is relevant to the task at hand." *Daubert*, 509 U.S.at 597. It is the Government's burden to persuade the Court that the answer is likely "yes." *See* Fed. R. Evid. 702 advisory committee note (2000) ("[T]he proponent has the burden of establishing that the pertinent admissibility requirements are met by a preponderance of the evidence"). But exclusion remains the exception, *see id.*, as "[v]igorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence," *Daubert*, 509 U.S. at 596.

The basis for Calhoun's second argument, that Hess' testimony relies on an untested theory, is a single case: *United States v. Evans*, 892 F. Supp. 2d 949 (N.D. Ill. 2012). There, the Government sought to rely upon the testimony of a cell-site expert to show that the criminal defendant, Antonio Evans, was in the area where a kidnapping took place. *Id.* at 951. The court explained that the theory of granulization involved (1) identifying the cell tower, sector, and sector-coverage direction used by the phone during the relevant time period; (2) estimating "the range of each [sector's] coverage based on the proximity of the tower to other towers in the area," and (3) predicting "where the coverage area of one tower will overlap with the coverage area of another." *Id.* at 952. Applying this theory to the facts at hand, the Government's expert intended to testify that Evans' cell-phone used two towers at the time of the kidnapping and that "[t]he building where the victim was held [fell] squarely within the coverage overlap of [those] two towers." *Id.* The court found one significant problem was that the expert's coverage-overlap

theory assumed that Evans' phone "used the towers closest to it at the time of the calls" without accounting for the possibility that Evans' might have connected to other towers because of signal obstruction or network traffic. *Id.* at 956. "Second," the court reasoned, "the granulization theory remains wholly untested by the scientific community, while other methods of historical cell site analysis can be and have been tested by scientists." *Id.* "Given that multiple factors [could] affect the signal strength of a tower and that [the expert's] chosen methodology ha[d] received no scrutiny outside the law enforcement community," the court concluded that the Government had not carried its burden in establishing that the granulization method was reliable. *Id.* at 957.

Hess' proposed testimony is not similar enough to that excluded in *Evans* to justify that result here. The Government explains that it "is not attempting to put a particular cell phone in [a] very specific location via Agent Hess' testimony"; instead, it "is attempting to show how the four phones in question originated in the Philadelphia, Pennsylvania [*sic*] on April 21, 2014, traveled in a similar pattern over the next few days, were in the Grand Rapids and West Bloomfield areas around the time of the robberies, and traveled back to Philadelphia on April 22-23, 2014." (Gov't Resp. to Mot. to Exclude at 10.) The Government "concedes" that cell-site data cannot place Defendants "in a precise location." (*Id.* at 11.) Thus, to the extent that Hess' testimony essentially consists of placing the four cell phones at issue in this case within a general geographic region, i.e., within a couple miles of a particular tower, the Court is not persuaded that Hess' testimony is based on the granulization theory or that *Evans* is on point.

As for testimony more akin to Hess'—that, because a log shows that a particular phone connected to a particular tower at a particular time, it can be inferred that a phone was within that tower's coverage area at that time—a number of courts have found such testimony to be based on reliable methods. *See, e.g.*, *United States v. Schaffer*, 439 F. App'x 344, 347 (5th Cir. 2011)

(finding that agent's testimony demonstrated that determining a phone's location based on cell-site data is "neither untested nor unestablished"); *United States v. Reynolds*, No. 12-20843, 2013 WL 2480684, at *5 (E.D. Mich. June 10, 2013) ("Testimony about cellular phone technology and the ability to determine the general area where calls are placed and received has been widely accepted by federal courts." (citing cases)); *United States v. Jones*, 918 F. Supp. 2d 1, 5 (D.D.C. 2013) ("[T]he use of cell phone location records to determine the general location of a cell phone has been widely accepted by numerous federal courts" (citing cases)). The Court finds these authorities persuasive. And to the extent that Hess has made assumptions about signal strength that call into question his estimate of where the phones were located at particular times, Defendants can test those assumptions on cross exam. *United States v. Freeman*, No. 06-20185, 2015 WL 2062754, at *5 (E.D. Mich. May 4, 2015) ("The fact that an expert did not take into account various factors that may affect the signal strength of a tower or impact its coverage range does not render the fundamental methodology of cell site analysis unreliable. Instead, the absence of those considerations goes to the weight of the testimony rather than its admissibility, and those considerations can be addressed through vigorous cross-examination." (internal quotation marks and citation omitted)).

As for Calhoun's argument that the Court cannot even tell if Hess' testimony is based on reliable methods because the Government's Rule 16 letter lacks sufficient disclosure, the Court mostly disagrees. As explained at the outset, at a basic level, Hess' method is straightforward: a cell phone has to connect to a cell tower to make a cellular communication; the cell tower is fixed somewhere (e.g., the roof of a building); the cell tower has a limited coverage area; and the service provider logs the connection (which phone, which tower, and when). This basic method is adequately disclosed in Hess' "Basic Princip[le]s Utilized in Record Analysis." (Apr. 6, 2015

Letter from Graveline to Defendants' Counsel at 3.) In particular, Hess explains that "[t]he tower with the best signal is the one the handset will use for service, this is the serving cell and will be used to make and receive calls," that each cell tower "has its own unique identifier, this identifier is used to track which towers the handsets use," that towers can be "located anywhere (church steeples, water towers, [etc.])," and that some service providers' logs show both the tower a phone used to initiate a call and the one used when the call ended. (*Id*.) This information, at least when coupled with publicly available information in any number of cases involving using cell-site data, sufficiently discloses Hess' method so that the Court can determine its reliability and fulfill its gatekeeper duties under Rule 702 and *Daubert*.

It appears that Calhoun's real complaint with the Government's Rule 16 disclosure is that Hess did not disclose the "source" of certain assertions. (Mot. to Exclude Expert at 5.) The following are among Hess' assertions that Calhoun complains of: even if the phone has a better signal to a tower different than the one providing service, "the phone will not randomly reselect to an adjacent tower unless the tower is on its 'neighbor list' which is controlled by the network service provider"; "[a]s the phone moves, it will choose a new serving cell based on signal strength and neighbor list"; a cell tower can be located anywhere; there are more towers in urban areas than in rural ones; and "[a] typical cell tower has THREE, 120° sectors." (Apr. 6, 2015 Letter from Graveline to Defs.' Counsel at 3; *see* Mot. to Exclude Expert at 5.) Calhoun says that Hess has not disclosed "any source for these so-called 'principals.'" (Mot. to Exclude Expert at 5.)

On this limited point the Court agrees with Calhoun. Although Federal Rule of Criminal Procedure 16 does not require detailed disclosure, *United States v. Campbell*, No. 1:04-CV-0424-RWS, 2006 WL 346446, at *1 (N.D. Ga. Feb. 13, 2006), it does demand that the

Government "describe . . . the bases and reasons for [its expert's] opinions," Fed. R. Crim. P. 16, and, according to the accompanying advisory committee note, that description "should cover not only written and oral reports, tests, reports, and investigations, but any information that might be recognized as a legitimate basis for an opinion under Federal Rule of Evidence 703," Fed. R. Crim. P. 16 advisory committee note (1993). Indeed, at oral argument, counsel for the Government indicated that they would explore whether more detailed information could be provided. Thus, the Court will order that the Government supplement its Rule 16 disclosure to explain the source of Hess' "Basic Princip[le]s Utilized in Record Analysis."

IV.

For the reasons stated, the Court will not suppress the cell-site data that the Government intends to introduce at trial. Although it may ultimately become settled that long-term tracking via cell phones, or the identification of a cell phone in a home, requires a warrant supported by probable cause, that law was not established at the time the Government sought and obtained the cell-site data at issue in this case. Deterrence, therefore, will not be forwarded by suppression. Calhoun's "Motion to Suppress Cell Site Location Information" (Dkt. 56) is DENIED.

The Court GRANTS IN PART Calhoun's "Motion to Exclude or Limit Expert Testimony, or, in the Alternative, for Additional Discovery" (Dkt. 53). In particular, the Government shall supplement its Rule 16 disclosure to inform Defendants (and the Court) of the sources of Hess' assertions in his "Basic Princip[le]s Utilized in Record Analysis." Calhoun's motion to exclude is otherwise DENIED WITHOUT PREJUDICE.

SO ORDERED.

s/Laurie J. Michelson
LAURIE J. MICHELSON
UNITED STATES DISTRICT JUDGE

Dated: July 31, 2015

CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the foregoing document was served on the attorneys and/or parties of record by electronic means or U.S. Mail on July 31, 2015.

s/Jane Johnson
Case Manager to
Honorable Laurie J. Michelson